

Rec'd PCT/PTO 07 DEC 2004
PCT/JP03/07541
13.06.03

日本国特許庁
JAPAN PATENT OFFICE

10/517258

REC'D 01 AUG 2003

WIPED PAT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2002年 6月14日

出願番号
Application Number: 特願2002-174883
[ST. 10/C]: [JP2002-174883]

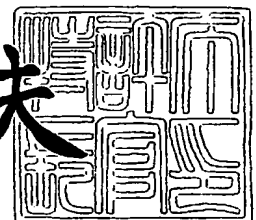
出願人
Applicant(s): 松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 7月11日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3056683

【書類名】 特許願

【整理番号】 2037840026

【提出日】 平成14年 6月14日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 12/14

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 難波 剛

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 中井 勝博

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 平野 雄久

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式
 会社内

 【氏名】 手塚 智明

【特許出願人】

 【識別番号】 000005821

 【氏名又は名称】 松下電器産業株式会社

【代理人】

 【識別番号】 100081813

 【弁理士】

 【氏名又は名称】 早瀬 憲一

 【電話番号】 06(6395)3251

【手数料の表示】

【予納台帳番号】 013527

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9600402

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 半導体集積回路装置

【特許請求の範囲】

【請求項 1】 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第 2 の格納手段を半導体集積回路内に有し、該第 2 の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第 1 の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記第 2 の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、

上記第 2 の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第 1 の格納手段からの上記書き換えプログラムを、上記第 2 の格納手段の外部読出し不可能領域に格納するようにした、

ことを特徴とする半導体集積回路装置。

【請求項 2】 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第 2 の格納手段を半導体集積回路内に有し、該第 2 の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第 1 の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記第 2 の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えた、

ことを特徴とする半導体集積回路装置。

【請求項 3】 請求項 2 に記載の半導体集積回路装置において、

上記制御回路は、上記第 2 の格納手段の特定のアドレスにある書き換えプログラムののみを読み出すように制御するものとした、

ことを特徴とする半導体集積回路装置。

【請求項 4】 請求項 2 に記載の半導体集積回路装置において、
上記制御回路は、上記第 2 の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとした、
ことを特徴とする半導体集積回路装置。

【請求項 5】 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第 2 の格納手段を半導体集積回路内に有し、該第 2 の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第 1 の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、

上記第 2 の格納手段に格納した上記書き換えプログラムの一部を実行する、
ことを特徴とする半導体集積回路装置。

【請求項 6】 請求項 5 に記載の半導体集積回路装置において、
上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである、
ことを特徴とする半導体集積回路装置。

【請求項 7】 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第 2 の格納手段を半導体集積回路内に有し、該第 2 の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第 1 の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第 1 の格納手段から上記第 2 の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えた、

ことを特徴とする半導体集積回路装置。

【請求項 8】 半導体集積回路内の演算処理ユニットにコンテンツを処理す

る動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、

上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、

上記第2の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、

上記第2の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行う、

ことを特徴とする半導体集積回路装置。

【請求項9】 請求項8に記載の半導体集積回路装置において、

上記第2の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとした、

ことを特徴とする半導体集積回路装置。

【請求項10】 請求項9に記載の半導体集積回路装置において、

上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用する、

ことを特徴とする半導体集積回路装置。

【請求項11】 請求項8に記載の半導体集積回路装置において、

上記第2の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次2分割した構成とし、該2分割した各々の領域に同じプログラムデータを格納するものであり、

上記チェックプログラムは、上記2分割した両領域の各々に格納された同じプ

ログラムデータを比較して正誤を判定するプログラムと、

前回の判定結果が正しいと判定されたときに、前回 2 分割した領域の 1 方の領域を、プログラムが格納されていない領域としてさらに 2 分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、

上記第 2 の格納手段に格納すべきプログラムすべてを順次格納する、

ことを特徴とする半導体集積回路装置。

【請求項 1 2】 請求項 1 1 に記載の半導体集積回路装置において、

上記第 2 の格納手段は、該第 2 の格納手段の上記書き換えプログラムが格納されていない領域を順次 2 分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとした、

ことを特徴とする半導体集積回路装置。

【請求項 1 3】 請求項 1 2 に記載の半導体集積回路装置において、

上記一意に得られるデータが、該プログラムデータの反転データである、

ことを特徴とする半導体集積回路装置。

【請求項 1 4】 請求項 8 ないし 1 3 のいずれかに記載の半導体集積回路装置において、

上記チェックプログラムを予め格納した ROM (Read Only Memory) を備え、

上記 ROM により上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行う、

ことを特徴とした半導体集積回路装置。

【請求項 1 5】 請求項 1 ないし 1 4 のいずれかに記載の半導体集積回路装置において、

上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、

上記第 1 の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第 2 の格納手段に復号化した上記書き換えプログラムを格納する、

ことを特徴とする半導体集積回路装置。

【請求項 16】 半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、

上記半導体集積回路内に、上記第1の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第2の格納手段に転送する復号化手段と、

上記第2の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、

上記暗号化手段で暗号化された書き換えプログラムと上記第1の格納手段に保持している暗号化された書き換えプログラムとを比較する、

ことを特徴とする半導体集積回路装置。

【請求項 17】 請求項 11ないし 13、及び 16のいずれかに記載の半導体集積回路装置において、

上記第2の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第1の格納手段に保持した書き換えプログラムを修正可能とした、

ことを特徴とする半導体集積回路装置。

【請求項 18】 請求項 1ないし 17のいずれかに記載の半導体集積回路装置において、

当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能とした、

ことを特徴とする半導体集積回路装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は半導体集積回路装置に関するものであり、特に、内容が第三者へ漏洩

したくない機密情報であるプログラムの保護に関するものである。

【0002】

【従来の技術】

DSPやCPUなどの演算処理ユニットを含む半導体集積回路において、演算処理ユニットのプログラムは、コスト面やプログラムの機密性を保つという点においてはROMとしてプログラムを格納することが有利となる。しかしながら、ROMなどの書き換え不可能な手段でプログラムを保持した場合、仕様変更やプログラム自身の不具合に柔軟な対応が取りにくい。このような回路の開発における容易さなどの点から、プログラムを半導体集積回路内部に格納する手段をRAMなどの書き換え可能な手段として所有することがある。このような構成を持つ回路においては、DSPやCPUのような信号処理・機器の制御を担う演算処理ユニットなどに必要なプログラムを事前に書き換え可能なRAMなどの指定領域にダウンロードする必要があった。

【0003】

しかし、DSPやCPUなどの演算処理ユニットのプログラムを外部からRAMにダウンロードする半導体集積回路においては、プログラムを半導体集積回路内部にROMで持っている場合よりもプログラムの内容が第三者に漏洩する危険が高いという欠点を有していた。

例えば、半導体集積回路外部に保持するプログラムが著作権保護を目的として策定されたウォーターマーク（電子透かし）を検出するためのプログラムのような場合、プログラムの内容が悪意を持った第三者に漏洩したことによって、著作権保護のための仕組みを無効化される恐れがあるため、プログラム自身を保護する必要がある。

この場合、半導体集積回路内にダウンロードするプログラムを予め暗号化させて、該半導体集積回路内で復号化させることにより、プログラム自身を保護することが考えられる。

【0004】

【発明が解決しようとする課題】

しかしながら、この予め暗号化したデータ、及び非暗号化データも含めて半導

体集積回路内の書き換え可能な領域にダウンロードしたプログラムデータが正しく格納できたか否かを、機密性を保持しながら確認することは困難である。

本発明はこのような問題を解決するためになされたものであり、機密性を要するプログラムデータを外部に漏らすことなく、正しくダウンロードできたか否かを確認できる半導体集積回路装置を提供することを目的とする。

【0005】

【課題を解決するための手段】

上記問題を解決するために、本発明の請求項1に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第2の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、上記第2の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第1の格納手段からの上記書き換えプログラムを、上記第2の格納手段の外部読出し不可能領域に格納するようにしたものである。

【0006】

これにより、例えばダミーデータなどを、上記第2の格納手段の読み出し可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、半導体集積回路内に正しく上記書き換えプログラムが格納されたかどうかを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0007】

また、本発明の請求項2に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納

手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第2の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えたものである。

【0008】

これにより、上記第2の格納手段に格納された特定部分のみを読み出して、該特定部分を検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0009】

また、本発明の請求項3に記載の半導体集積回路装置は、請求項2に記載の半導体集積回路装置において、上記制御回路は、上記第2の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するものとしたものである。

【0010】

これにより、上記第2の格納手段の特定のアドレスのみを読み出して、該特定のアドレスのデータを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0011】

また、本発明の請求項4に記載の半導体集積回路装置は、請求項2に記載の半導体集積回路装置において、上記制御回路は、上記第2の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとしたものである。

【0012】

これにより、上記第2の格納手段の特定のビットのみを読み出して、該特定のビットのみを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持し

ながら確認することができる。

【0013】

また、本発明の請求項5に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、上記第2の格納手段に格納した上記書き換えプログラムの一部を実行するものである。

【0014】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0015】

また、本発明の請求項6に記載の半導体集積回路装置は、請求項5に記載の半導体集積回路装置において、上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものである。

【0016】

これにより、例えば、上記第2の格納手段に格納された上記書き換えプログラムの先頭プログラムと最終プログラムとを実行した場合、該書き換えプログラムが最後まで正しく格納できたかを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0017】

また、本発明の請求項7に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理

する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第1の格納手段から上記第2の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えたものである。

【0018】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0019】

また、本発明の請求項8に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラムが含まれたものであり、上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、上記第2の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、上記第2の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行うものである。

【0020】

これにより、接続切り換え手段にて演算処理ユニットのプログラム入力またはデータ入力を切り替えて、上記書き換えプログラムのデータを取り込んで、例えば該書き換えプログラムデータのチェックサムなどをもって、予め決めておいた値と比較することが可能になるので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該

書き換えプログラムの機密を保持しながら確認することができる。

【0021】

また、本発明の請求項9に記載の半導体集積回路装置は、請求項8に記載の半導体集積回路装置において、上記第2の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとしたものである。

【0022】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第2の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

【0023】

また、本発明の請求項10に記載の半導体集積回路装置は、請求項9に記載の半導体集積回路装置において、上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用するものである。

【0024】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第2の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

【0025】

また、本発明の請求項11に記載の半導体集積回路装置は、請求項8に記載の半導体集積回路装置において、上記第2の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次2分割した構成とし、該2分割した各々の領域に同じプログラムデータを格納するものであり、上記チェックプログラムは、上記2分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、前回の判定結果が正しいと判定されたときに

、前回 2 分割した領域の 1 方の領域を、プログラムが格納されていない領域としてさらに 2 分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、上記第 2 の格納手段に格納すべきプログラムすべてを順次格納するものである。

【0026】

これにより、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第 2 の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる。

【0027】

また、本発明の請求項 12 に記載の半導体集積回路装置は、請求項 11 に記載の半導体集積回路装置において、上記第 2 の格納手段は、該第 2 の格納手段の上記書き換えプログラムが格納されていない領域を順次 2 分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとしたものである。

【0028】

これにより、例えば、第 2 の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第 2 の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第 2 の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

【0029】

また、本発明の請求項 13 に記載の半導体集積回路装置は、請求項 12 に記載の半導体集積回路装置において、上記一意に得られるデータが、該プログラムデータの反転データであるものとしたものである。

【0030】

これにより、例えば、第 2 の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致

し、上記第2の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第2の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる。

【0031】

また、本発明の請求項14に記載の半導体集積回路装置は、請求項8ないし13のいずれかに記載の半導体集積回路装置において、上記チェックプログラムを予め格納したROM (Read Only Memory) を備え、上記ROMにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行うものである。

【0032】

これにより、上記チェックプログラムの転送誤り等により、チェックプログラムが機能しなくなるのを防ぎ、上記第2の格納手段に上記書き換えプログラムが正しく格納できたか否かを確認するチェックプログラムを安定的に提供することができる効果がある。

【0033】

また、本発明の請求項15に記載の半導体集積回路装置は、請求項1ないし14のいずれかに記載の半導体集積回路装置において、上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、上記第1の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第2の格納手段に復号化した上記書き換えプログラムを格納するものである。

【0034】

これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0035】

また、本発明の請求項16に記載の半導体集積回路装置は、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格

納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第1の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第2の格納手段に転送する復号化手段と、上記第2の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、上記暗号化手段で暗号化された書き換えプログラムと上記第1の格納手段に保持している暗号化された書き換えプログラムとを比較するものである。

【0036】

これにより、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる。

【0037】

また、本発明の請求項17に記載の半導体集積回路装置は、請求項11ないし13、及び16のいずれかに記載の半導体集積回路装置において、上記第2の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第1の格納手段に保持した書き換えプログラムを修正可能としたものである。

【0038】

これにより、第2の格納手段において正しく格納できなかった箇所を使用しないように書き換えプログラムを修正して書き込むので、メモリを有効に活用することができる。

【0039】

また、本発明の請求項18に記載の半導体集積回路装置は、請求項1ないし17のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたものである。

【0040】

これにより、書き換えプログラムを半導体集積回路装置外部に有する場合にお

いても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる。

【0041】

【発明の実施の形態】

以下、本発明の実施の形態について、図を用いて説明する。

(実施の形態1)

図1は、本発明の実施の形態1に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

【0042】

図において、100は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、105は制御用マイコン、101はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）である。半導体集積回路109は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）102と、書き換え可能なRAM（第2の格納手段）108と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ107の処理を行う演算処理回路（演算処理ユニット）106とから構成される。

【0043】

また、本発明の実施の形態1に係る半導体集積回路装置において、書き換え可能なRAM108は、半導体集積回路109の外部から読み出し可能な外部読み出し可能領域103と、半導体集積回路109の外部から読み出し不可能な外部読み出し不可能領域104とから構成される。

【0044】

以上のように構成された半導体集積回路装置100について、図2のフローチャートを用いてその動作を説明する。

制御用マイコン105の制御にしたがい、暗号化されていないデータを書き換え可能なRAM108の外部読み出し可能領域103に入力する（ステップS201）。次に、外部読み出し可能領域103に入力したデータが正しいかを半導体集

積回路 109 外部に読み出して制御用マイコン 105 等でチェックする（ステップ S202）。ステップ S202 でチェックした結果が正しい場合に、制御用マイコン 105 の制御にしたがいメモリ 101 の暗号化された書き換えプログラムを復号化回路 102 に入力し（ステップ S203）、暗号化された書き換えプログラムを復号する（ステップ S204）。次に、ステップ S204 で復号化された書き換えプログラムを書き換え可能な RAM 108 の外部読出し不可能領域 104 に入力する（ステップ S205）。以上の処理により、第三者に漏洩したくない書き換えプログラムの機密性を保ちながら、該書き換えプログラムが正しく格納されているか否かをチェックすることができる。

なお、書き換え可能な RAM 109 の外部読出し可能領域 103 に格納するデータは、半導体集積回路装置の内部、及び外部のどちらに用意してもよく、チェック用のデータであればよい。

【0045】

以上のような、本発明の実施の形態 1 に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムを書き換え可能な RAM 108 に入力する場合に、該 RAM 108 に設けた外部読出し可能領域 103、及び外部読出し不可能領域 104 のうち、外部読み出し可能領域 103 にチェック用のデータを格納し、該データのチェックの結果が正しいと判定された後、外部読出し不可能領域 104 に該機密情報のプログラムを格納することにより、第三者に漏洩したくない機密情報である書き換えプログラムを格納した RAM 108 の製造上の欠陥、及び入力するまでの経路のチェックをすることができる。

【0046】

（実施の形態 2）

本発明の実施の形態 2 に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムの機密性を保ちながら、該書き換えプログラムが半導体集積回路内の書き換え可能な RAM に正しく格納されているかを確認するために、格納した書き換えプログラムの特定部分のみを半導体集積回路に読み出すように制御する制御回路を備えたものである。

【0047】

図3は、本発明の実施の形態3に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

図において、300は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であり、301は制御用マイコン、303はあらかじめ暗号化された書き換えプログラムを格納しているメモリ（第1の格納手段）である。半導体集積回路308は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）302と、復号化回路302で復号した書き換えプログラムを格納するための書き換え可能なRAM（第2の格納手段）304と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ307の処理を行う演算処理回路（演算処理ユニット）305と、RAM304に格納された書き換えプログラムのうち特定アドレスのみ出力するように制御する制御回路306とから構成される。

【0048】

次に、以上のように構成された半導体集積回路装置300について、図4のフローチャートを用いて動作を説明する。

暗号化された書き換えプログラムを格納するメモリ303からの該書き換えプログラムを復号化回路302で復号し（ステップS401）、該復号化した書き換えプログラムをRAM304に inputs（ステップS402）。次に、制御回路306から、RAM304に格納されている書き換えプログラムの特定アドレスの読み出しを行い（ステップS403）、該特定アドレスのプログラムを半導体集積回路308外部に読み出してチェックする（ステップS404）。

【0049】

以上のような本発明の実施の形態2に係る半導体集積回路装置は、書き換えプログラムをRAM304に格納した後、特定のアドレスのみを半導体集積回路外部に読み出すように制御する制御回路を備え、該読み出された特定アドレスをチェックすることにより、第三者に漏洩したくない機密情報である書き換えプログラムがRAM304に正しく格納されたかどうかを、該書き換えプログラムの機密性を保持しながら判断することができる。

【0050】

なお、本実施の形態 2 では特定アドレスのみを読み出し可能としたが、特定ビットのみを半導体集積回路外部に読み出すように制御し、該読み出した特定ビットをチェックしても、書き換えプログラムが RAM に格納されたかどうか判断することができる。

【0051】

(実施の形態 3)

本発明の実施の形態 3 に係る半導体集積回路装置は、第三者に漏洩したくない機密情報の書き換えプログラムが半導体集積回路内の書き換え可能な RAM に正しく格納されているかを判断するために、該半導体集積回路の RAM に格納した書き換えプログラムの一部を実行するものである。

図 5 は、本発明の実施の形態 3 に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムをダウンロードする例を示す。

【0052】

図において、500 は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、501 は制御用マイコン、503 は、あらかじめ暗号化された書き換えプログラムを格納しているメモリ（第 1 の格納手段）である。半導体集積回路 507 は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）502 と、復号化回路 502 で復号化された書き換えプログラムを格納するための書き換え可能な RAM（第 2 の格納手段）504 と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ 506 の処理を行う演算処理回路（演算処理ユニット）505 とから構成される。

【0053】

本実施の形態 3 において、上記あらかじめ暗号化された書き換えプログラムには、ダウンロード後に該書き換えプログラムの一部を実行するプログラムが含まれているものとする。

【0054】

次に、以上のように構成された半導体集積回路 500 について、図 6 のフローチャートを用いてその動作を説明する。

メモリ 503 からの暗号化した書き換えプログラムを復号化回路 502 で復号し (ステップ S601)、該復号した書き換えプログラムを RAM 504 に入力する (ステップ S602)。次に、RAM 504 に格納した書き換えプログラムの一部を実行させ (ステップ S603)、正しいか否かが判断されたら、半導体集積回路 507 外部に正しいか否かを通知する信号を出力する (ステップ S604)。

このとき、実行するプログラムの内容を例えばメモリチェックなどのプログラムにし、該メモリチェックを実行させ、そのチェックの結果が得られたならば、RAM 504 に正しくプログラムが格納されているかの判断をより確実に行える。

【0055】

また、図 7 のように、実行するプログラムの内容を、JUMP 命令などを実行して非連続領域のプログラムを実行するプログラムにし、例えば、先頭プログラムでメモリチェックのプログラムのアドレス XX に JUMP する命令を実行するとする。そして、先頭プログラムからメモリチェックのプログラムのアドレス XX に JUMP して、メモリチェックを行うようにすることにより、RAM 504 に正しくプログラムが格納されているかの判断をより確実に行える。また、先頭プログラムで最終プログラムのアドレス YY に JUMP する命令を実行するとする。そして先頭プログラムから最終プログラムのアドレス YY に JUMP して、該最終プログラムは、該最終プログラムを実行後にアドレス 01 に戻るようなプログラムにして、その結果、プログラムが正しく実行されたことを確認することにより、書き換えプログラムが RAM の最後まで書きこまれているかどうかを判断することができ、特に、暗号化を間違えると後段のデータに影響を及ぼす暗号化方式においては、書き換えプログラムが正しく格納されているかをより一層確実に判断できる。

【0056】

以上のような本発明の実施の形態 3 に係る半導体集積回路装置は、書き換えプログラムを RAM 504 に格納した後、該書き換えプログラムの一部を実行し、正しく実行できた場合に信号を出力することによって、書き換えプログラムが R

AMに正しく格納できたかどうかを判断することができる。

【0057】

また、書き換えプログラムを格納したRAM504から、非連続なプログラム領域を順次実行することにより、書き換えプログラムが最後までRAMに正しく格納されたかを確認することが可能になり、RAMに格納した書き換えプログラムの正誤チェックを、より確実に行うことができる。

【0058】

(実施の形態4)

本発明の実施の形態4に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しく格納されているかを確認するために、半導体集積回路内のRAMに書き換えプログラムを書き込む際に、転送データを監視する転送監視回路を備え、転送されるデータ単位ごとの算術和をとって結果を保持し、チェックサムなどをとるようにしたものである。

【0059】

図8は、本発明の実施の形態4に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

図において、801は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、802はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、803は制御用のマイコンである。半導体集積回路810は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）805と、復号化回路805で復号化された書き換えプログラムを格納するためのRAM（第2の格納手段）806と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ807の処理を行う演算処理回路（演算処理ユニット）808と、復号化回路805から転送されるデータ単位ごとの算術和をとる転送監視回路（転送監視手段）809とから構成される。

【0060】

次に、本発明の実施の形態4に係る半導体集積回路装置の動作を説明する。

以上のように構成された半導体集積回路装置 801 において、あらかじめ暗号化されメモリ 802 に格納された書き換えプログラムを、制御用マイコン 803 の制御のもと、復号化回路 805 をととして復号しながら RAM 806 に格納する。この時、同時に、データ転送用のデータパスの一部である復号化回路 805 から RAM 806 への信号線を転送監視回路 809 が常に監視し、転送されるデータ単位ごとの算術和をとって結果を保持していく。そして、メモリ 802 に格納されたデータのうちあらかじめ決められたデータ量の転送が終了した時点で、転送監視回路 809 に保持されている算術和のデータを読み出し、制御用マイコン 803 において、あらかじめ計算しておいた正しく転送がおこなわれたときのデータの算術和と比較し、同じ値であれば転送が正しくおこなわれたと判断し、その後、本来実行すべき処理を行う。もし、この両者の値が異なっていれば、正しく転送がおこなわれなかったと判断し、メモリ 802 に入っているデータを再度転送し直すなど、しかるべき処置を施す。

【0061】

以上のような本発明の実施の形態 4 に係る半導体集積回路装置は、書き換えるための書き換えプログラムの転送データを監視し、転送されるデータ単位ごとの算術和をとる転送監視回路を備え、該転送監視回路でとった算術和と、あらかじめ計算しておいた正しく転送が行われたときのデータの算術和とを比較するので、第三者に漏洩したくない機密情報である書き換えプログラムを読み出すことなく、正しくダウンロードされたか否かを判断することができる。

【0062】

なお、本実施の形態 4 では、データ転送監視回路を用いてチェックサムをとる例を説明したが、チェックサムの代わりに CRC チェック回路、ECC チェック回路など、データのあるかたまり単位でビット誤りがあるか否かが判定できるものであれば同様の効果を得ることができ、特にこの監視方式を限定するものではない。

【0063】

(実施の形態 5)

本発明の実施の形態 5 に係る半導体集積回路装置は、第三者に漏洩したくない

機密情報である書き換えプログラムが、半導体集積回路に正しく格納されているか否かを確認するために、演算処理回路のワークメモリから該演算処理回路を動作させることと、RAMに格納されたプログラムデータを演算処理回路に入力させることとを可能にし、演算処理回路にて、チェックサムなどをとるようにしたものである。

【0064】

図9は、本発明の実施の形態5に係る半導体集積回路装置を示す図であり、暗号化された書き換えプログラムを半導体集積回路内に格納する例を示す。

図において、901は、暗号化された書き換えプログラムをもつ半導体集積回路装置であって、902はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、903は制御用のマイコンである。半導体集積回路915は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）905と、復号化回路905で復号化された書き換えプログラムを格納するためのRAM（第2の格納手段）906と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ907の処理を行う演算処理回路（演算処理ユニット）908と、演算処理回路908のワークメモリ911と、RAM906、及びワークメモリ911のそれぞれを、演算処理回路908の命令プログラムを読み込むバス913、及びデータを入出力するバス914に接続できるように切り替える接続切り替え回路（接続切り替え手段）912とから構成されている。また、本実施の形態5において、RAM906と演算処理回路908の命令プログラムを読み込むバス913とが接続され、ワークメモリ911とデータを入出力するバス914とが接続される形態を第1の形態とし、また、RAM906とデータを入出力するバス914とが接続され、ワークメモリ911と演算処理回路908の命令プログラムを読み込むバス913とが接続される形態を第2の形態とし、接続切り替え回路912は、上記第1、及び第2の形態のいずれかの形態に切り替えるものである。通常の状態では、上記第1の形態を取るものとし、これらの構成により、演算処理回路908は、自分自身の命令プログラムを読み込むバス913とデータを読み込むバス914とは独立しているいわゆるハーバードアーキテクチャを取ることができ、より高速に

コンテンツデータ 907 に対するデータ処理が実行できるものである。

【0065】

次に、本発明の実施の形態 5 に係る半導体集積回路装置 901 の動作を説明する。

あらかじめ暗号化されメモリ 902 に格納された書き換えプログラムを制御用マイコン 903 の制御のもと、復号化回路 905 をとおして復号しながら RAM 906 に格納する。その後、演算処理回路 908 の動作を開始する。このとき演算処理回路 908 は、RAM 906 の中の書き換えプログラムに組み込まれた実行ステップに応じて動作する。

【0066】

また、この RAM 906 に格納された書き換えプログラムの中に、書き換えプログラムが RAM 906 に正しく格納できたか否かをチェックするプログラム（チェックプログラム）を予め組み込んでおく。本実施の形態 5 では、データを入力するバス 914 上の RAM 906 のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することにより RAM 906 に格納されているデータが正しいことを判定するようなプログラムと、正しいと判断された後に接続切り替え回路 912 を第 1 の形態に戻すように切り替えるプログラムとの上記 2 つのプログラムをマシン語データとして組み込んでおき、さらに、該組み込んだマシン語データを直接ワークメモリ 911 に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路 912 を第 2 の形態に切り替えるプログラムとを書き換えプログラムの中に予め組み込んでおく。

【0067】

そして、動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ 911 に展開するプログラムにより、上記マシン語データである、上記 RAM 906 に格納されたプログラムが正しいか否かを判定するための上記 2 つのプログラムがワークメモリ 911 に展開される。その後、上記接続切り替え回路 912 を第 2 の形態に切り替えるプログラムによって、接続切り替え回路 912 を第 2 の形態に切り替える。これにより、ワークメモリ 911 と、

演算処理回路 908 の命令プログラムを読み込むバス 913 とが接続されるため、演算処理回路 908 はワークメモリ 911 に先ほど展開した上記 2 つのプログラムのうち、データを入出力するバス 914 上の RAM 906 のデータを読み込み、たとえばチェックサムをとってあらかじめ決められた値と比較することにより RAM 906 に格納されているデータが正しいことを判定するようなプログラムを実行する。これにより、RAM 906 に格納されている書き換えプログラムが正しいと判定されれば、上記ワークメモリ 911 に展開した 2 つのプログラムの残りのプログラムである、接続切り替え回路 912 を第 1 の形態に戻すように切り替えるプログラムを実行することによって、接続切り替え回路 912 は第 1 の形態に切り替えられ、以後本来実行すべきプログラムを実行する。

【0068】

次に、RAM 906 を図 10 のような構成にした例を説明する。

この RAM 906 は、図 10 に示すような論理的構成をとるものである。a2400、a2401、a2402 は、メモリアドレスを示しており、右上がり斜線ハッチをつけたアドレス a2400 で始まり、アドレス a2401 で終わる空間に書き換えプログラムを格納する。また、アドレス a2401 で始まり、アドレス a2402 で終わる空間には、上記右上がり斜線ハッチをつけたアドレス a2400 で始まりアドレス a2401 で終わる空間に格納されたデータの、たとえばメモリアドレスごとなどのように、あらかじめ決められた単位ごとに対する、たとえばパリティフラグを格納するものとする。

【0069】

そして、RAM 906 に格納する書き換えプログラムの中にあらかじめ組み込んでおくチェックプログラムとして、データを入出力するバス 914 上の RAM 906 のデータを読み込み、該読み込んだデータの中の 1 のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムと、さらに前記読み込んだデータに対応するアドレス a2401 から a2402 の空間に格納されているパリティフラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較してメモリ 2406 に格納された書き換えが正しいか否かを判断するプログラムと、正しいと判断された後

に接続切り替え回路 912 を第 1 の形態に戻すように切り替えるプログラムとの上記 3 つのプログラムをマシン語データとして組み込んでおき、さらに、該組み込んだマシン語データを直接ワークメモリ 911 に展開するプログラムと、上記マシン語データをワークメモリに展開した後、接続切り替え回路 912 を第 2 の形態に切り替えるプログラムとを予め組み込んでおく。

【0070】

動作を開始した後、まず、上記予め組み込んでおいたマシン語データを直接ワークメモリ 911 に展開するプログラムにより、上記マシン語データである、上記 3 つのプログラムがワークメモリ 911 に展開される。その後、上記接続切り替え回路 912 を第 2 の形態に切り替えるプログラムによって、接続切り替え回路 912 を第 2 の形態に切り替える。これにより、ワークメモリ 911 と演算処理回路 908 の命令プログラムを読み込むバス 913 とが接続されるため、演算処理回路 908 はワークメモリ 911 に先ほど展開した上記 3 つのプログラムのうち、データを入出力するバス 914 上のメモリのデータを読み込み、該読み込んだデータの中の 1 のビットが奇数個あるか偶数個あるかということを数えるいわゆるパリティ演算をおこなうプログラムを実行し、次に、前記読み込んだデータに対応するアドレス a2401 から a2402 の空間に格納されているパリティフラグの情報を読み込んだ後に、該パリティフラグの情報、及び上記パリティ演算結果の両者を比較して RAM 906 に格納された書き換えプログラムが正しいか否かを判断するプログラムを実行する。これにより正しいと判断されれば、上記ワークメモリ 911 に展開した 3 つのプログラムの残りのプログラムである、接続切り替え回路 912 を第 1 の形態に戻すように切り替えるプログラムによって、接続切り替え回路 912 は第 1 の状態に切り替られ、以後本来実行すべきプログラムを実行する。

【0071】

このように、RAM 906 を上記構成にすることにより、RAM 906 に格納した書き換えプログラムが正しく格納されたか否かを確認することができるとともに、書き換えプログラムが正しく格納できていない場合、該正しく格納できていない場所の情報を得ることができる。

【0072】

なお、RAM906のアドレスa2401からa2402までの空間に入れるデータは、パリティフラグに限らず、データのあるかたまりで正しいか否かが判定できるものであればよく、現在よく知られているものにCRCチェックやECCチェックなどがあり、これらを使用しても同様の効果が得られる。

【0073】

以上のような本発明の実施の形態5に係る半導体集積回路装置は、RAM906に格納された書き換えプログラムが正しく格納されているかを確認するためのチェックプログラムを演算処理回路のワークメモリ911に展開し、接続切り替え回路912を切り替えて、ワークメモリ911からの命令を可能にし、該ワークメモリ911からの命令を受けた演算処理回路にて、チェックサムなどをとることにより、第三者に漏洩したくない機密情報である書き換えプログラムがRAM906に正しく格納されているか否かを、機密性を保持しながら確認することができる。

【0074】

なお、本発明の実施の形態5に係る半導体集積回路装置では、演算処理回路でチェックサムをとる例を説明したが、チェックサムの代わりにCRCチェック回路、ECCチェック回路など、データのあるかたまり単位でビットに誤りがあるか否かが判定できるものであれば同様の効果を得ることができる。

【0075】

(実施の形態6)

本発明の実施の形態6に係る半導体集積回路装置は、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路に正しく格納されたか否かの確認を安定して行うために、RAMに格納された書き換えプログラムが正しいか否かの確認をするためのチェックプログラムを予めROMに格納して、該ROMに格納したチェックプログラムによって、上記書き換えプログラムの確認動作を行うものである。

【0076】

図11は、本発明の実施の形態6に係る半導体集積回路装置を示す図であり、

暗号化された書き換えプログラムを半導体集積回路内にダウンロードする例を示す。

図において、1101は暗号化された書き換えプログラムをもつ半導体集積回路装置であって、1102はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、半導体集積回路1116は、制御用のマイコン1103と、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）1105と、復号化回路1105で復号化した書き換えプログラムを格納するためのRAM（第2の格納手段）1106と、復号化したプログラムの制御手順に従って動作し、コンテンツデータ1107の処理を行う演算処理回路（演算処理ユニット）1108と、演算処理回路1108のワークメモリ1111と、RAM1106、及びワークメモリ1111のそれぞれを、演算処理回路1108の命令プログラムを読み込むバス1113、及びデータを入出力するバス1114に接続できるように切り替える接続切り替え回路（接続切り替え手段）1112と、演算処理回路1108によって実行できるRAM1106に展開された書き換えプログラムが正しいか否かを判定するためのプログラム（チェックプログラム）を格納したROM1115とから構成され、ROM1115は、常に演算処理回路1108の命令プログラムを読み込むバス1113に接続される。また、接続切り替え回路1112によって切り替える第1、及び第2の形態は実施の形態5と同様なので説明を省略する。また、実施の形態5と同様、通常の状態では、上記第1の形態を取るものとする。

【0077】

次に、本発明の実施の形態6に係る半導体集積回路装置の動作を説明する。

まず最初に、あらかじめ暗号化されメモリ1102に格納された書き換えプログラムを制御用マイコン1103の制御のもと、復号化回路1105をとおして復号しながらRAM1106に格納する。その後、演算処理回路1108の動作を開始する。この時、切り替え回路1112は、第1の形態になるよう接続されているものとする。演算処理回路1108は、RAM1106の中に展開された書き換えプログラムの実行ステップに応じて動作する。この書き換えプログラムの中に、ROM1115の中にあるデータチェック用のプログラムに制御を移す

ようなプログラムがあり、これを実行する。そして、演算処理回路 1108 の実行プログラムが ROM 1115 に移った後、接続切り替え回路 1112 を第 2 の形態になるように切り替える。

【0078】

これにより、RAM 1106 とデータを入出力するバス 1114 とが接続されるため、演算処理回路装置 1108 は、ROM 1115 に格納されている、RAM 1106 に展開された書き換えプログラムが正しいか否かを判断するプログラムに従い、RAM 1106 のデータを読み込み、かつ正しいかどうかの判断をする。

正しいと判断されれば、ROM 1115 に組み込まれている接続切り替え回路 1112 を第 1 の形態に戻すように切り替えるプログラムによって、接続切り替え回路 2512 は第 1 の状態に切り替られ、以後本来実行すべきプログラムを実行する。

【0079】

なお、RAM 1106 に格納されている書き換えプログラムが正しいか否かを確認する方法は、ROM 1115 に実装されている方式によるが、この方式には、たとえばチェックサムなどが用いられる。しかしながら、必ずしも方式を限定するものではなく、データのある決められた固まり単位で正しいことが判定できればよいことは言うまでもない。

【0080】

次に、RAM 1106 を図 12 のような構成にした場合について説明する。

図 12 は、本発明の実施の形態 6 に係る半導体集積回路装置の RAM 1106 の例を示したものである。

図において、a2600、a2601、a2602、a2603、a2604 は、メモリアドレスを示しており、a2600 は RAM 1106 におけるスタートアドレスを示し、a2604 はエンドアドレスを示す。また、右上がり斜線ハッチをつけて示すように、a2601 は RAM 1106 の全容量のちょうど半分に位置する場所のアドレスを示している。また、右下がり斜線をつけて示すように、a2602 はアドレス a2601 とエンドアドレス a2604 とであらわさ

れた容量のちょうど半分に位置する場所のアドレスを示す。同様に、a 2 6 0 3 はアドレス a 2 6 0 2 とエンドアドレス a 2 6 0 4 とであらわされる容量のちょうど半分に位置するアドレスを示している。

【0081】

以上のような RAM 1 1 0 6 を用いた半導体集積回路装置 1 1 0 1 の動作について説明する。

まず最初に、RAM 1 1 0 6 のアドレス a 2 6 0 0 から a 2 6 0 1 までの部分にメモリ 1 1 0 2 から復号化回路 1 1 0 5 を通してデータをダウンロードする。そのあと、アドレス a 2 6 0 1 から a 2 6 0 4 までの領域にも、RAM 1 1 0 2 に格納されている先に展開したアドレス a 2 6 0 0 から a 2 6 0 1 までのデータと全く同じデータを、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路 1 1 1 2 を切り替えて RAM 1 1 0 6 のデータを読み出す。この読み出し時に、アドレス a 2 6 0 0 からとアドレス a 2 6 0 1 からとのそれぞれ等距離にあるものを順次アクセスし、得られたデータのビットごとの排他的論理和を取る。暗号が正しく解け、データパスに異常がなく、かつ、RAM 1 1 0 6 の格納域ビットに異常がなければ、この排他的論理和の結果は、あるデータと同じデータとの排他的論理和となるため、0 になる。したがって、この手順を準次繰り返し、各排他的論理和が 0 であることを確かめれば、メモリ 1 1 0 2 から復号化回路 1 1 0 5 を通して RAM 1 1 0 6 に正しく展開できているという判断ができる。上記手順を残り領域の 1/2 ずつ繰り返し実行することで、RAM 1 1 0 6 には、演算処理回路 1 1 0 8 のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

【0082】

このように、RAM 1 1 0 6 を上記構成にすることにより、何らかの不具合のために、上記手順の排他的論理和が 0 とならない場合には、RAM 1 1 0 6 に格納されているデータに不具合があると判断できるとともに、不具合発生アドレスも知ることができる。

なお、メモリ 1 1 0 2 から RAM 1 1 0 6 に展開するデータ量は、RAM 1 1 0 6 の書き換えプログラムが格納されていない領域の 1/2 以下ずつであればよ

いが、排他的論理和をとる上記方法においては、1/2が読み出し可能な最大データ量であるので、1/2とすることで書き込み効率を大きくとれる。

【0083】

また、本実施の形態6において、このように構成されたRAM1106を用いて、データチェックプログラムROM1115に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムROM1115がない場合でも、実施の形態5のように、ダウンロードするプログラムに予めデータチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

【0084】

次に、メモリ1102の構成を図13のような構成にした場合について説明する。

図13は、本発明の実施の形態6に係る半導体集積回路装置におけるメモリ1102の例を示したものである。

【0085】

図において、a2710、a2711、a2712、a2713、a2714、a2715、a2716、a2717は、メモリ1102におけるアドレスを示している。アドレスa2710は、メモリ1102のスタートアドレスを示し、アドレスa2717は、メモリ1102のエンドアドレスを示す。また、アドレスa2710とアドレスa2711に囲まれた空間には、図12で示したRAM1106のアドレスa2600からa2601に入るべきデータを暗号化して格納する。便宜上これを「データA」と呼ぶ。また、アドレスa2711とアドレスa2712に囲まれた空間には、復号化回路1105によって復号化するとRAM1106のアドレスa2600からa2601に入るべきデータ、即ち「データA」を各ビットごとに反転したものが得られるようなデータが格納される。これを便宜上「データA'」と呼ぶ。同様に、アドレスa2712とアドレスa2713に囲まれた空間には、RAM1106のアドレスa2601からa2602に入るべきデータを暗号化したものを格納し、アドレスa2713とアドレスa2714に囲まれた空間には、復号化回路1105によって復号化すると

RAM1106のアドレスa2601からa2602に入るべきデータを各ビットごとに反転したものが得られるようなデータが格納される。これらを便宜上それぞれ、「データB」「データB'」と呼ぶ。「データC」及び「データC'」も同様の対応である。このような手順を繰り返し、RAM1106に格納すべき全てのプログラム及びその反転データを上記手順に従って、暗号化してメモリ1102に格納する。

【0086】

以上のように構成されたメモリ1102、及びRAM1106を使った半導体集積回路装置1101の動作について説明する。

まず、RAM1106のアドレスa2600からa2601までの部分にメモリ1102から復号化回路1105を通して「データA」をダウンロードする。そのあと、上記手順にて述べたメモリ1102に格納されている今ダウンロードしたデータの反転データを暗号化したものである「データA'」を、これも同様に復号化しながらダウンロードする。この後、接続切り替え回路1112を切り替えてRAM1106のデータを読み出す。この読み出し時に、アドレスa2600からとアドレスa2601からとのそれぞれ等距離にあるものを順次アクセスし、得られたデータのビットごとの論理積を取る。暗号が正しく解け、データパスに異常がなく、かつ、RAM1106の格納域ビットに異常がなければ、この論理積の結果は、あるデータとその反転データとの論理積となるため、0になる。したがって、この手順を順次繰り返し、各論理積が0であることをたしかめれば、メモリ1102から復号化回路1105を通してRAM1106に正しく展開できているということになる。メモリ1102には、RAM1106の各手順における残りの領域の1/2ずつのデータとその反転データが暗号化されて「データB」「データB'」「データC」「データC'」などのように対になって必要な量だけ格納されており、上記手順を残り領域の1/2ずつデータがなくなるまで繰り返し実行することで、RAM1106には、演算処理回路1108のプログラムが復号化されてダウンロードされ、同時に、そのデータ内容が期待どおりであることが確かめられる。

【0087】

これにより、もしも何らかの不具合のために、上記手順の論理積が0とならない場合に、RAM1106に格納されているデータに不具合があると判断できるとともに、不具合発生アドレスも知ることができる。また、何らかの理由により、復号化回路1105に不具合がありRAM1106への出力が固定値になっていても、RAM2506に格納されているデータを上記手順で論理積をとれば、あるデータと同じデータの論理積であるため、0にはならない。このことで、正しくデータが格納されてはいないと判断できる。

【0088】

なお、メモリ1102からRAM1106に展開するデータ量は、該RAM1106の残り領域の1/2以下ずつであってもよいが、論理積をとる上記方法においてはRAM1106の残り領域の1/2が読み出し可能な最大データ量であるので、1/2とすることで書き込み効率を大きくとれる。

【0089】

また、本実施の形態6において、このように構成されたメモリ1102を用いて、データチェックプログラムROM1115に格納されたプログラムに基づいてデータチェックを行う例を説明したが、データチェックプログラムROM1115がない場合でも、実施の形態5のように、ダウンロードする書き換えプログラムに予めチェックプログラムを組み込むようにすることにより同様の効果を得ることができる。

【0090】

以上のような本発明の実施の形態6に係る半導体集積回路装置は、RAM1106に格納されている書き換えプログラムが正しく格納されているか否かを確認するためのチェックプログラムをROM化したメモリ1115に格納したので、チェックプログラムの転送や、展開に誤りが発生しても、RAM1106に格納された書き換えプログラムが正しく格納できたか否かの確認を、容易に、かつ、安定して行うことができる。

【0091】

また、RAM1106の書き換えプログラムが格納されていない領域を2分割した各々の領域に、該書き換えプログラムが格納されていない領域の1/2に相

当するプログラムデータと、該 1/2 の領域に読み出したプログラムデータと同じデータとを順次読み出し、該読み出したそれぞれのデータから排他的論理和をとる手順を繰り返し行うようにしたので、RAM 1106 に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、書き換えプログラムが RAM 1106 に正しく格納できていない場合に、RAM 1106 における正しく格納できていない場所の情報を得ることができる。

【0092】

また、RAM 1106 の書き換えプログラムが格納されていない領域を 2 分割した各々の領域に、該書き換えプログラムが格納されていない領域の 1/2 に相当するプログラムデータと、該 1/2 の領域に読み出したプログラムデータを反転したデータとを順次読み出し、該読み出したそれぞれのデータから論理積をとる手順を繰り返し行うようにしたので、RAM 1106 に格納された書き換えプログラムが正しく格納されたかを確認することができるとともに、何らかの理由により復号化回路 1105 の不具合で RAM 1106 への出力が固定値になり、排他的論理和をとってもデータが一致し、上記第 2 の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、RAM 1106 に格納したプログラムの正誤を正しく判別できる。

【0093】

なお、本発明の実施の形態 1～6 に係る半導体集積回路装置では、予め暗号化した書き換えプログラムを、半導体集積回路内にダウンロードする例を説明したが、暗号化されていない書き換えプログラムを半導体集積回路内にダウンロードしても同様の効果が得られるのはいうまでもない。

【0094】

(実施の形態 7)

本発明の実施の形態 7 に係る半導体集積回路装置は、予め暗号化された書き換えプログラムをメモリに格納した半導体集積回路装置において、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納されたか否かを、該書き換えプログラムの機密性を保持しながら確認するために、上記暗号化された書き換えプログラムを復号して RAM に格納した後、該書き換えプログラムを再度

暗号化し、該再度暗号化したプログラムデータと、上記予め暗号化されたプログラムデータとを比較するようにしたものである。

【0095】

図14は、本発明の実施の形態7に係る半導体集積回路装置の構成を示す図である。

図において、1401は暗号化された書き換えプログラムをもつ半導体集積回路装置であり、1402はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第1の格納手段）であり、1403は制御用のマイコンである。半導体集積回路1411は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）1405と、復号化回路で復号された書き換えプログラムを格納するためのRAM（第2の格納手段）1406と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ1407の処理を行う演算処理回路（演算処理ユニット）1408と、上記RAM1406に転送されたデータを再度暗号化する暗号化回路（暗号化手段）1410とから構成される。

【0096】

次に、以上のように構成された半導体集積回路装置1401の動作を説明する。

まず、あらかじめ暗号化されメモリ1402に格納された書き換えプログラムを制御用マイコン1403の制御のもと、復号化回路1405をとおして復号しながらRAM1406に格納する。そして、メモリ1402に格納されたデータのうち、あらかじめ決められたデータ量の転送が終了した時点で、今度は、制御用マイコン1403の制御のもと、今復号化してメモリ1406に格納した書き換えプログラムを読み出し、暗号化回路1410を通して再度暗号化し、該再度暗号化したプログラムデータとメモリ1402に格納されている予め暗号化したプログラムデータとを比較する。この両者のデータが一致すれば、最初にメモリ1402から読み出し、復号化回路1405にて復号化し、RAM1406に格納した書き換えプログラムが、正しいと判断できる。

【0097】

以上のような、本発明の実施の形態 7 に係る半導体集積回路装置は、予め暗号化したプログラムを半導体集積回路 1411 にダウンロードする半導体集積回路装置において、暗号化した書き換えプログラムを復号化し、RAM 1406 に格納した後、暗号化回路 1410 で再度暗号化し、予め暗号化した書き換えプログラムと再度暗号化した書き換えプログラムとを比較するようにしたので、第三者に漏洩したくない機密情報の書き換えプログラムをそのまま外部に読み出すことなく、RAM 1406 に格納した書き換えプログラムが正しく格納できたか否かを確認することができる。

【0098】

(実施の形態 8)

本発明の実施の形態 8 に係る半導体集積回路装置は、RAM に格納した書き換えプログラムが正しくないと判定された場合、該書き換えプログラムの修正箇所を検出して書き換えプログラムを修正可能にしたものである。

以下、本発明の実施の形態 8 に係る半導体集積回路装置を、図 15、図 16、及び図 17 を用いて説明する。

【0099】

図 15 は、本発明の実施の形態 8 に係る半導体集積回路装置の構成を示した図であり、実施の形態 7 で説明した半導体集積回路装置において、RAM に格納されたプログラムが正しくないと判断された場合、プログラムを修正可能とする例を示したものである。

【0100】

図において、1500 は、暗号化された書き換えプログラムをダウンロードしてなる半導体集積回路装置であって、1503 はあらかじめ暗号化された書き換えプログラムが格納されているメモリ（第 1 の格納手段）であり、1501 は制御用のマイコンである。半導体集積回路 1509 は、暗号化された書き換えプログラムを復号化するための復号化回路（復号化手段）1502 と、復号化回路 1502 で復号された書き換えプログラムを格納するための RAM（第 2 の格納手段）1504 と、復号化されたプログラムの制御手順に従って動作し、コンテンツデータ 1508 の処理を行う演算処理回路（演算処理ユニット）1505 と、

RAM1504に格納された書き換えプログラムを再度暗号化する暗号化回路1506とから構成される。ここまでの構成は図14の半導体集積回路装置1401と同じであるが、半導体集積回路装置1500においては、暗号化回路1506の出力S1506とあらかじめ暗号化された書き換えプログラムが格納されているメモリ1503の出力S1503とを比較し、RAM1504に正しく格納されなかった場所を検出する比較器1507を備えている。

【0101】

以上のように構成された半導体集積回路装置1500について、以下にその動作を説明する。図16は、実施の形態8に係る半導体回路1500の動作フローを示す。

まず、暗号化した書き換えプログラムを復号化回路1502で復号し（ステップS1601）、制御用マイコン1501にしたがい、復号化した書き換えプログラムをRAM1504に入力する（ステップS1602）。ステップS1602でRAM1504に入力した書き換えプログラムを暗号化回路1506で再度、暗号化し（ステップS1603）、ステップS1603で暗号化した書き換えプログラムとメモリ1503に保持している書き換えプログラムとを比較する（ステップS1604）。ステップS1604でのチェックで正しくない場合、制御用マイコン1501に従って、正しくない部分のRAMのビットを使用しないように書き換えプログラムを修正する（ステップS1605）。そして、ステップS1605で修正したプログラムを復号化し（ステップS1606）、該復号化したプログラムをRAM1504に入力する（ステップS1607）。

【0102】

また、ステップS1605の書き換えプログラム修正の動作は、例えば、図17のように、RAM1504に格納された書き換えプログラムの正しくない部分が、例えばマシン語単位などあらかじめ決められた単位のアドレスXXからアドレスXX'とすると、アドレスXXからアドレスXX'に格納されるべきデータを修正プログラムとしてアドレスYYからアドレスYY'に格納するようにする。このとき、修正プログラムに、アドレスXXまで読み出したときにアドレスYYにJUMPする命令プログラムと、次にアドレスYY'まで読み出したときに

アドレス XX' に JUMP する命令プログラムとを組み込んでおくことにより、RAM 1504 に格納されたプログラムの読み出しを正常に行うことができる。

【0103】

これにより、上記方法によると、修正プログラムを RAM 1504 に入力した後、読み出してチェックすることにより RAM 1504 内の欠陥のあるビットを使わないようにできるため、RAM の有効活用ができる。

【0104】

なお、本実施の形態 8 では、予め暗号化した書き換えプログラムを格納するメモリ 1503 からの出力 S1503 と復号した書き換えプログラムを再度暗号化する暗号化回路 1506 からの出力 S1506 とを比較した結果から、RAM 1504 に正しく格納できなかった場所を検出して、書き換えプログラムを修正したが、上述した書き換えプログラムの修正は、RAM の欠陥位置を検出できれば可能であるので、実施の形態 6 で説明したメモリ、及び RAM の構成により読み出したデータの排他的論理和、及び論理積をとってデータをチェックする例においても適用可能である。

【0105】

以上のような、実施の形態 8 に係る半導体集積回路装置は、書き換えプログラムが RAM に正しく格納されたか否かを確認した結果、RAM に正しく格納されなかった場合に、正しく書き込めていない RAM のビットを使用しないように書き換えプログラムを修正して、RAM にダウンロードするので、RAM の一部のビットが正しく生成できていなくても、その他の部分に書き込んで、書き換えプログラムを正しく動作させることができ、RAM を有効に活用することができる。

【0106】

なお、本発明の実施の形態 1～8 の半導体集積回路装置では、書き換えプログラムをメモリ（第 1 の格納手段）に格納して、半導体集積回路内にダウンロードしたが、半導体集積回路装置外部に書き換えプログラムを保持し、例えば、インターネット等の通信手段を用いて、半導体集積回路内にダウンロードしても同様の効果を得ることができるのはいうまでもない。

【0107】

【発明の効果】

以上のような、本発明の請求項1に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第2の格納手段は、該半導体集積回路外部から読出しが可能な外部読出し可能領域と、読出しが不可能な外部読出し不可能領域とを有するものであり、上記第2の格納手段の外部読出し可能領域に任意のデータを入力格納したのち、該データを該半導体集積回路の外部に読出して、該任意のデータが上記入力した通りのデータであるかを確認し、そののち、上記第1の格納手段からの上記書き換えプログラムを、上記第2の格納手段の外部読出し不可能領域に格納するようにしたので、例えばダミーデータなどを、上記第2の格納手段の読み出し可能な領域に書き込んで、該書き込んだダミーデータを読み出してチェックをすることにより、半導体集積回路内に正しく上記書き換えプログラムが格納されたかどうかを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0108】

また、本発明の請求項2に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記第2の格納手段に格納された上記書き換えプログラムの特定部分のみを読み出すように制御する制御回路を備えたものとしたので、上記第2の格納手段に格納された特定部分のみを読み出して、該特定部分を検証することにより、上記

書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0109】

また、本発明の請求項3に係る半導体集積回路装置によれば、請求項2に記載の半導体集積回路装置において、上記制御回路は、上記第2の格納手段の特定のアドレスにある書き換えプログラムのみを読み出すように制御するもの、としたので、上記第2の格納手段の特定のアドレスのみを読み出して、該特定のアドレスのデータを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0110】

また、本発明の請求項4に係る半導体集積回路装置によれば、請求項2に記載の半導体集積回路装置において、上記制御回路は、上記第2の格納手段に格納した書き換えプログラムの特定のビットのみを読み出すように制御するものとしたので、上記第2の格納手段の特定のビットのみを読み出して、該特定のビットのみを検証することにより、上記書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0111】

また、本発明の請求項5に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、書き換え後に該プログラムの一部を実行するプログラムを含んだものであり、上記第2の格納手段に格納した上記書き換えプログラムの一部を実行するので、第三者に漏洩したくない機密情報である書き換えプ

プログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0112】

また、本発明の請求項6に係る半導体集積回路装置によれば、請求項5に記載の半導体集積回路装置において、上記実行する書き換えプログラムの一部は、非連続なプログラム領域を順次実行するものであるもので、例えば、上記第2の格納手段に格納した書き換えプログラムの先頭プログラムと最終プログラムとを実行した場合、該書き換えプログラムが最後まで正しく格納できたかを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0113】

また、本発明の請求項7に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第1の格納手段から上記第2の格納手段に転送される上記書き換えプログラムを監視する転送監視手段を備えたものとしたので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0114】

また、本発明の請求項8に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記書き換えプログラムは、プログラムの正誤の判定を行うチェックプログラ

ムが含まれたものであり、上記半導体集積回路内に、上記演算処理ユニットのワークメモリと、上記第2の格納手段または上記ワークメモリと、上記演算処理ユニットのプログラム入力またはデータ入力との接続を切り替える接続切り替え手段とを備え、上記第2の格納手段に格納された上記書き換えプログラムから抽出した上記チェックプログラムを上記ワークメモリに格納し、該ワークメモリに格納したチェックプログラムにより、上記演算処理ユニットを動作させ、上記書き換えプログラムの正誤チェックを行うので、接続切り換え手段にて演算処理ユニットのプログラム入力あるいはデータ入力を切り替えて、上記書き換えプログラムのデータを取り込んで、例えば該書き換えプログラムのデータのチェックサムなどをもって、予め決めておいた値と比較することが可能となり、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0115】

また、本発明の請求項9に記載の半導体集積回路装置によれば、請求項8に記載の半導体集積回路装置において、上記第2の格納手段は、上記書き換えプログラムを格納するとともに、該書き換えプログラムのうち、ある決められたかたまりから所定の法則に従い一意に得られるデータを格納するものとしたので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第2の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる効果がある。

【0116】

また、本発明の請求項10に係る半導体集積回路装置によれば、請求項9に記載の半導体集積回路装置において、上記一意に得られるデータを、上記プログラムの正誤チェックをするためのチェックコードとして使用するので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第2の格納手段に正しく格納できなかった場合

、正しく格納できていない場所の情報を得ることができる効果がある。

【0117】

また、本発明の請求項 11 に係る半導体集積回路装置によれば、請求項 8 に記載の半導体集積回路装置において、上記第 2 の格納手段は、その構成を、上記書き換えプログラムが格納されていない領域を順次 2 分割した構成とし、該 2 分割した各々の領域に同じプログラムデータを格納するものであり、上記チェックプログラムは、上記 2 分割した両領域の各々に格納された同じプログラムデータを比較して正誤を判定するプログラムと、前回の判定結果が正しいと判定されたときに、前回 2 分割した領域の 1 方の領域を、プログラムが格納されていない領域としてさらに 2 分割し、該分割した領域の各々に同じプログラムデータを格納する動作を繰り返すプログラムとを有し、上記第 2 の格納手段に格納すべきプログラムすべてを順次格納するので、第三者に漏洩したくない機密情報である書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができるとともに、上記第 2 の格納手段に正しく格納できなかった場合、正しく格納できていない場所の情報を得ることができる効果がある。

【0118】

また、本発明の請求項 12 に係る半導体集積回路装置によれば、請求項 11 に記載の半導体集積回路装置において、上記第 2 の格納手段は、該第 2 の格納手段の上記書き換えプログラムが格納されていない領域を順次 2 分割した各々の領域に、上記書き換えプログラムデータと、該プログラムデータから所定の法則に従い一意に得られるデータとを格納するものとしたので、例えば、第 2 の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第 2 の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第 2 の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる効果がある。

【0119】

また、本発明の請求項 13 に係る半導体集積回路装置によれば、請求項 12 に

記載の半導体集積回路装置において、上記一意に得られるデータが、該プログラムデータの反転データであるので、例えば、第2の格納手段の前段に復号化回路を備えて、該復号化回路の不具合により出力が固定値になり、排他的論理和をとってもデータが一致し、上記第2の格納手段に格納した書き換えプログラムが正しく格納できたか否かの確認が困難になる場合においても、第2の格納手段に格納した書き換えプログラムの誤りを容易に見つけ出すことができる効果がある。

【0120】

また、本発明の請求項14に係る半導体集積回路装置によれば、請求項8ないし13のいずれかに記載の半導体集積回路装置において、上記チェックプログラムを予め格納したROM (Read Only Memory) を備え、上記ROMにより上記演算処理ユニットを動作させて、上記書き換えプログラムの正誤チェックを行うので、上記チェックプログラムの転送誤り等により、チェックプログラムが機能しなくなるのを防ぎ、上記第2の格納手段に上記書き換えプログラムが正しく格納できたか否かを確認するチェックプログラムを安定的に提供することができる効果がある。

【0121】

また、本発明の請求項15に係る半導体集積回路装置によれば、請求項1ないし14のいずれかに記載の半導体集積回路装置において、上記半導体集積回路内に、暗号化された書き換えプログラムを復号する復号化手段を備え、上記第1の格納手段に格納された書き換えプログラムが予め暗号化されている場合、上記復号化手段は、該暗号化プログラムを復号化し、上記第2の格納手段に復号化した上記書き換えプログラムを格納するので、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0122】

また、本発明の請求項16に係る半導体集積回路装置によれば、半導体集積回路内の演算処理ユニットにコンテンツを処理する動作をさせるためのプログラムを、書き換え可能に格納する第2の格納手段を半導体集積回路内に有し、該第2

の格納手段に格納されたプログラムに対し、上記演算処理ユニットにコンテンツを処理する動作をさせるための、書き換え用である、予め暗号化された書き換えプログラムを格納する第1の格納手段を用いて書き換えを行うようにした半導体集積回路装置において、上記半導体集積回路内に、上記第1の格納手段からの上記暗号化された書き換えプログラムを復号化し、該復号化した書き換えプログラムを上記第2の格納手段に転送する復号化手段と、上記第2の格納手段に格納した書き換えプログラムを再度暗号化する暗号化手段とを備え、上記暗号化手段で暗号化された書き換えプログラムと上記第1の格納手段に保持している暗号化されたプログラムとを比較するので、第三者に漏洩したくない機密情報であり、また、予め暗号化されている書き換えプログラムが半導体集積回路内に正しくダウンロードできたか否かを、該書き換えプログラムの機密性を保持しながら確認することができる効果がある。

【0123】

また、本発明の請求項17に係る半導体集積回路装置によれば、請求項11ないし13、及び16のいずれかに記載の半導体集積回路装置において、上記第2の格納手段にデータが正しく格納されていない場合、不良箇所を検出し、上記第1の格納手段に保持した書き換えプログラムを修正可能としたので、第2の格納手段において、正しく格納できなかった箇所を使用しないように書き換えプログラムを修正して書き込むので、メモリを有効に活用することができる効果がある。

【0124】

また、本発明の請求項18に係る半導体集積回路装置によれば、請求項1ないし17のいずれかに記載の半導体集積回路装置において、当該半導体集積回路装置外部に保持した書き換えプログラムを、上記半導体集積回路内にダウンロード可能としたので、書き換えプログラムを半導体集積回路装置外部に有する場合においても、ネットワーク等の通信手段を用いてダウンロードでき、第三者に漏洩したくない機密情報である書き換えプログラムが正しく格納できたか否かを、機密性を保持しながら確認することができる効果がある。

【図面の簡単な説明】

【図 1】

本発明の実施の形態 1 における半導体集積回路装置を示す図

【図 2】

本発明の実施の形態 1 における半導体集積回路装置の動作を示すフローチャート

【図 3】

本発明の実施の形態 2 における半導体集積回路装置を示す図

【図 4】

本発明の実施の形態 2 における半導体集積回路装置の動作を示すフローチャート

【図 5】

本発明の実施の形態 3 における半導体集積回路装置を示す図

【図 6】

本発明の実施の形態 3 における半導体集積回路装置を示す図

【図 7】

本発明の実施の形態 3 における半導体集積回路の実行プログラムの一例を示す図

【図 8】

本発明の実施の形態 4 における半導体集積回路装置を示す図

【図 9】

本発明の実施の形態 5 における半導体集積回路装置を示すブロック構成図

【図 10】

本発明の実施の形態 5 における半導体集積回路装置の RAM（第 2 の格納手段）の構成の一例を示す構成図

【図 11】

本発明の実施の形態 6 における半導体集積回路装置を示すブロック構成図

【図 12】

本発明の実施の形態 6 における半導体集積回路装置の RAM（第 2 の格納手段）1106 の構成の一例を示す図

【図 13】

本発明の実施の形態 6 におけるメモリ 1102 内のデータ配置を示す概念図

【図 14】

本発明の実施の形態 7 における半導体集積回路装置を示すブロック構成図

【図 15】

本発明の実施の形態 8 における半導体集積回路装置を示すブロック構成図

【図 16】

本発明の実施の形態 8 における半導体集積回路装置の動作を示すフローチャート

【図 17】

本発明の実施の形態 8 における半導体集積回路装置のプログラムの修正を行う一例を示した図

【符号の説明】

100、300、500、801、901、1101、1401、1500
半導体集積回路装置

109、308、507、810、915、1116、1411、1509
半導体集積回路

101、303、503、802、902、1102、1402、1503
暗号化されたプログラムを格納しているメモリ（第 1 の格納手段）

105、301、501、803、903、1103、1403、1501
制御用のマイコン

102、302、502、805、906、1105、1405、1502
復号化回路（復号化手段）

108、304、504、806、906、1106、1406、1504
プログラムを格納する RAM（第 2 の格納手段）

103 プログラムを格納する RAM108 の外部読出し可能領域

104 プログラムを格納する RAM108 の外部読出し不可能領域

106、305、505、808、908、1108、1408、1505
演算処理回路（演算処理ユニット）

107、307、506、807、907、1107、1407、1508

コンテンツデータ

306 制御回路

809 転送監視回路 (転送監視手段)

911、1111、 ワークメモリ

912、1112 接続切り替え回路

913、1113 命令プログラムを読み込むバス

914、1114 データを入出力するバス

1115 データチェックプログラムROM

1506 暗号化回路 (暗号化手段)

S1503 暗号化されたプログラムを格納しているメモリ1503の出力信号

S1506 暗号化回路1506の出力信号

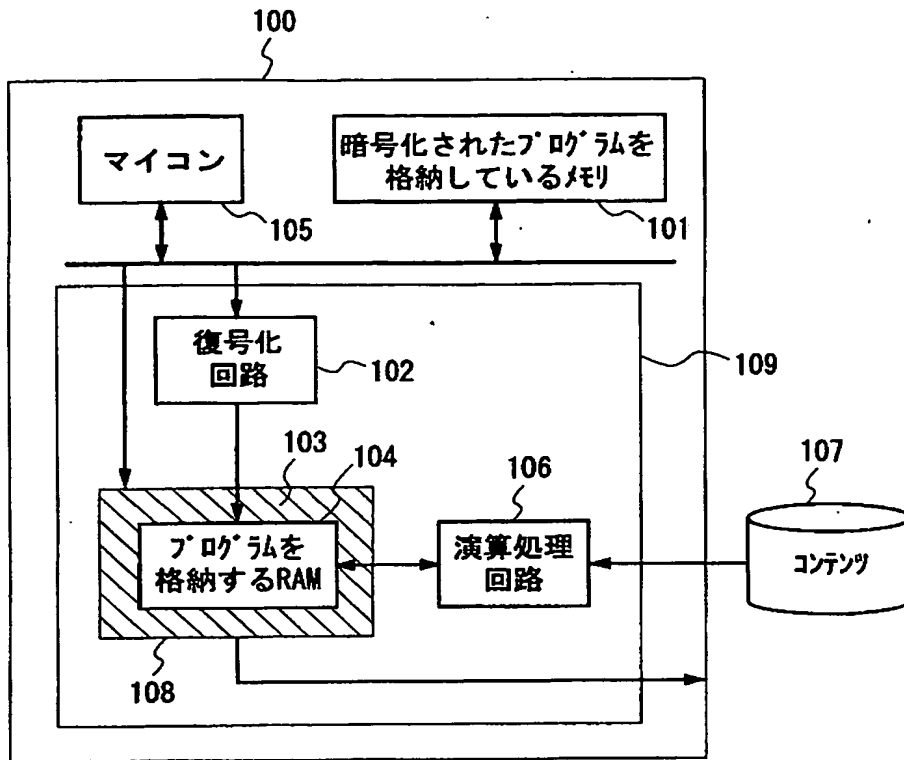
a2400～a2402 プログラムを格納するRAM906のアドレス

a2600～a2604 プログラムを格納するRAM1106のアドレス

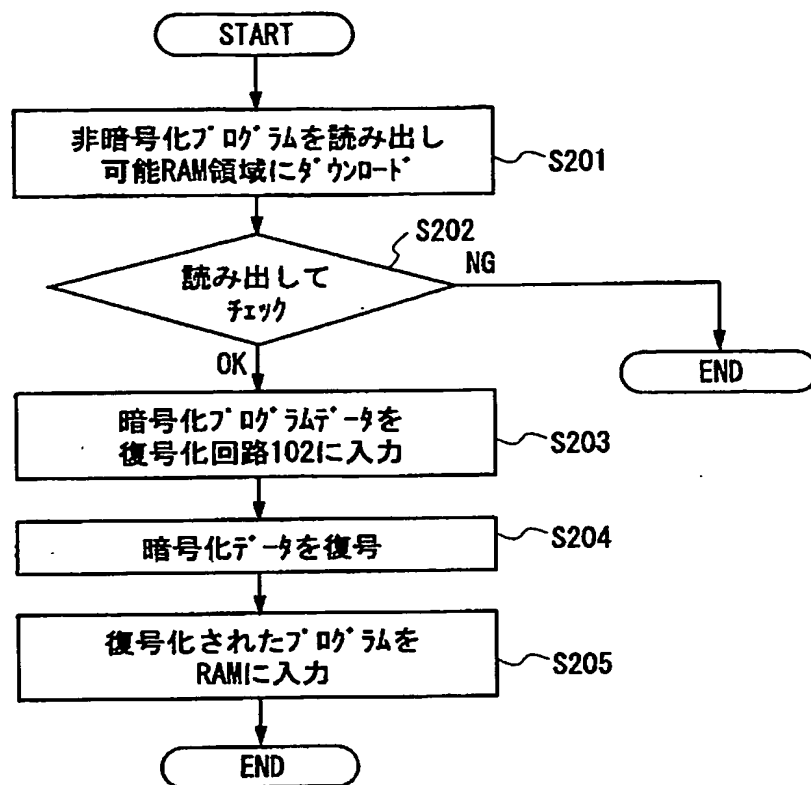
a2710～a2717 暗号化されたプログラムを格納するメモリ1102
のアドレス

【書類名】 図面

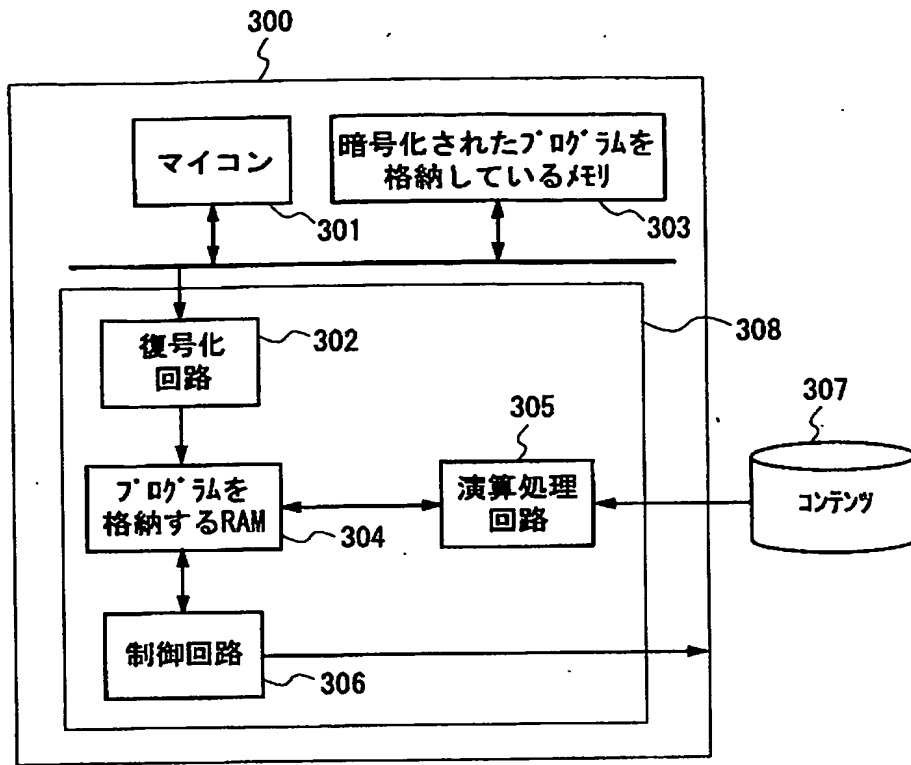
【図 1】



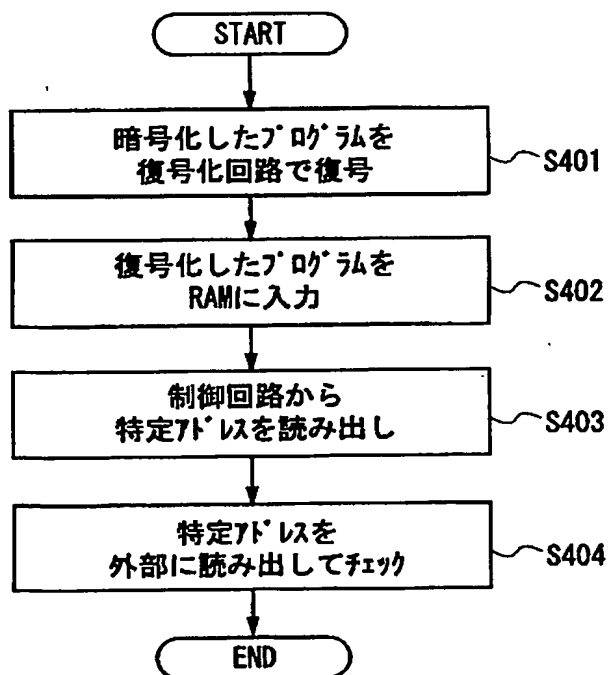
【図 2】



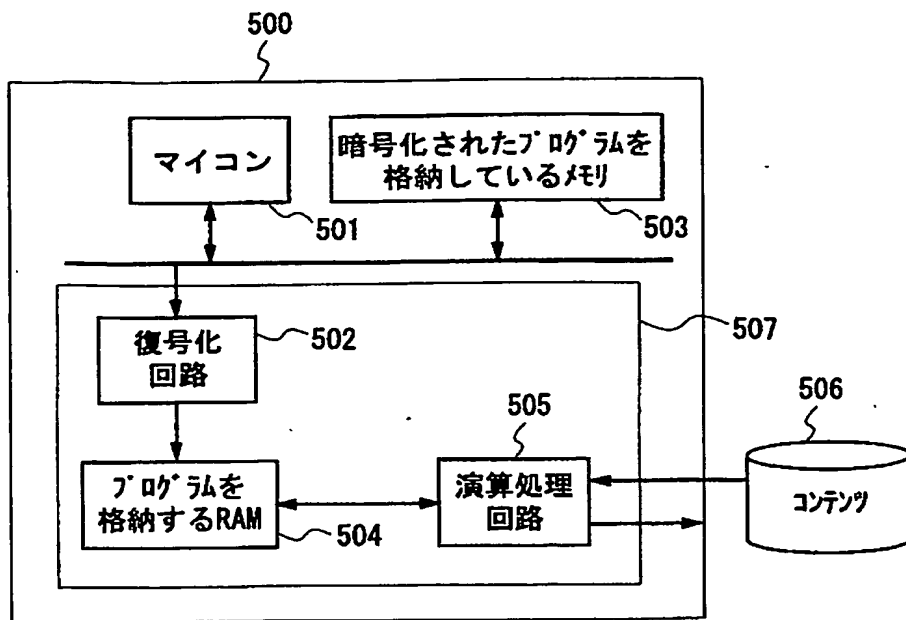
【図 3】



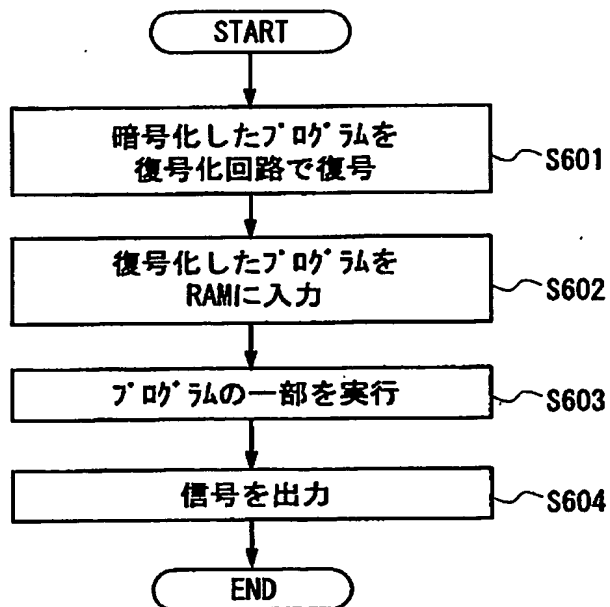
【図 4】



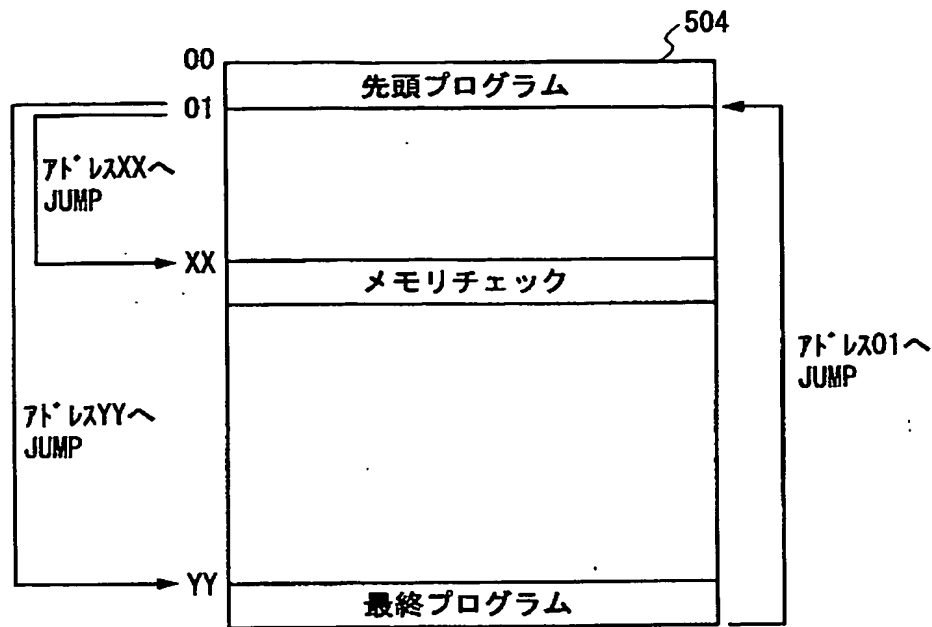
【図 5】



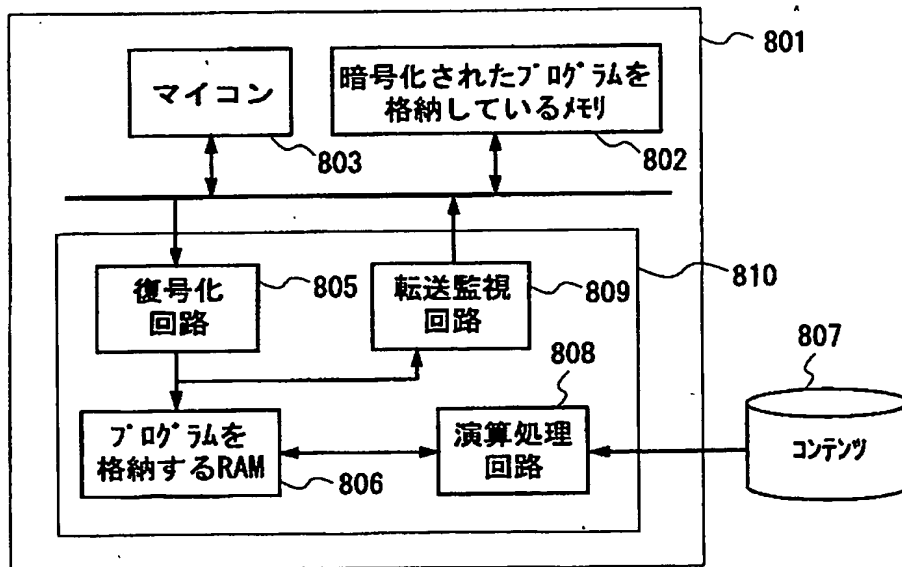
【図 6】



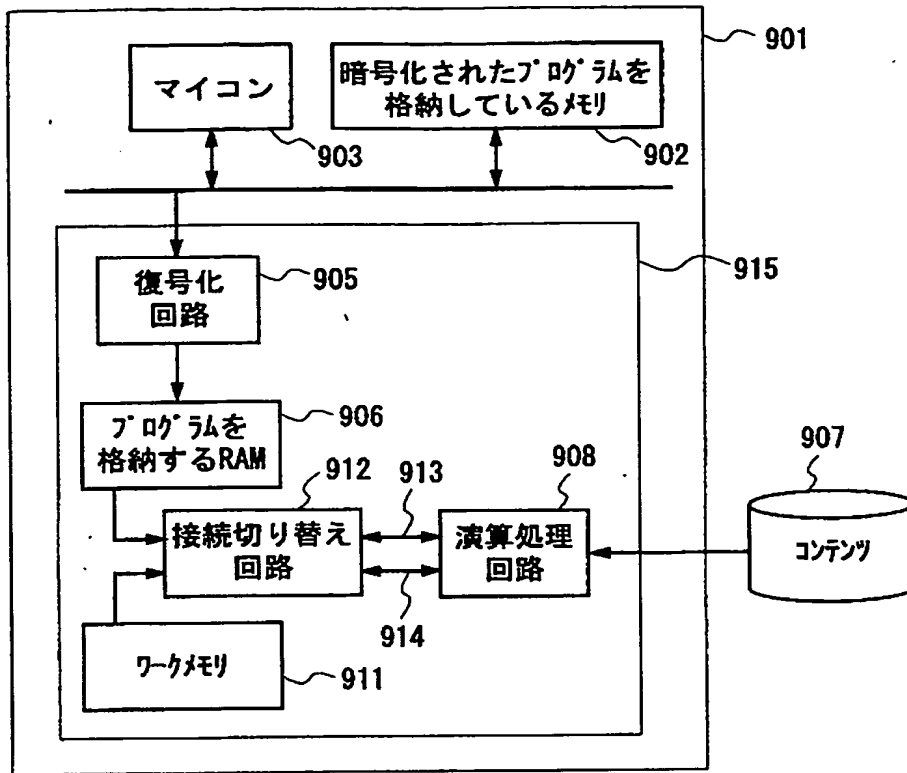
【図7】



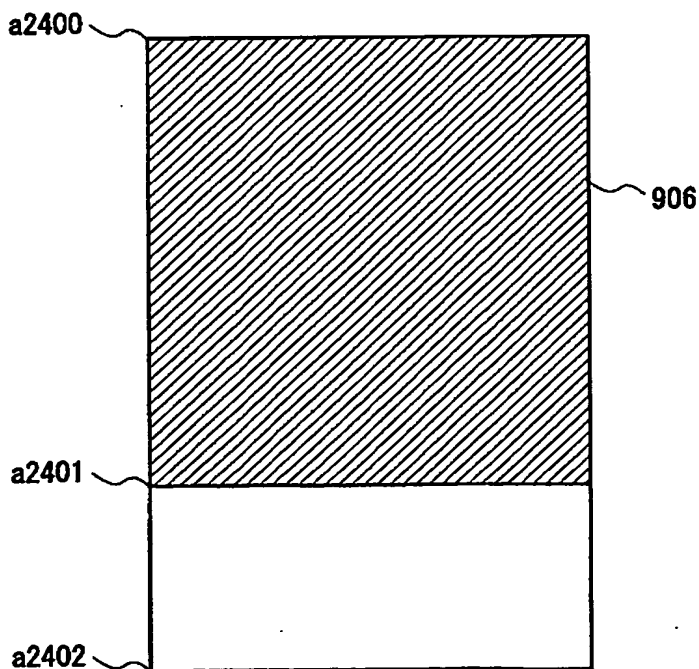
【図8】



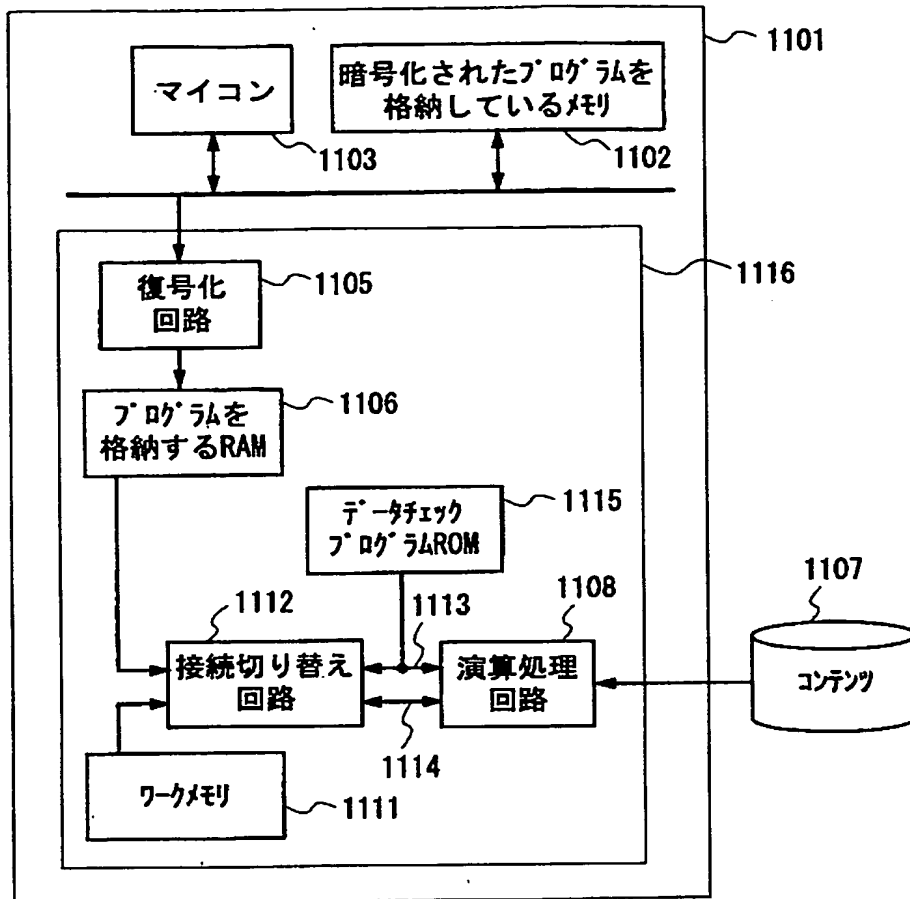
【図 9】



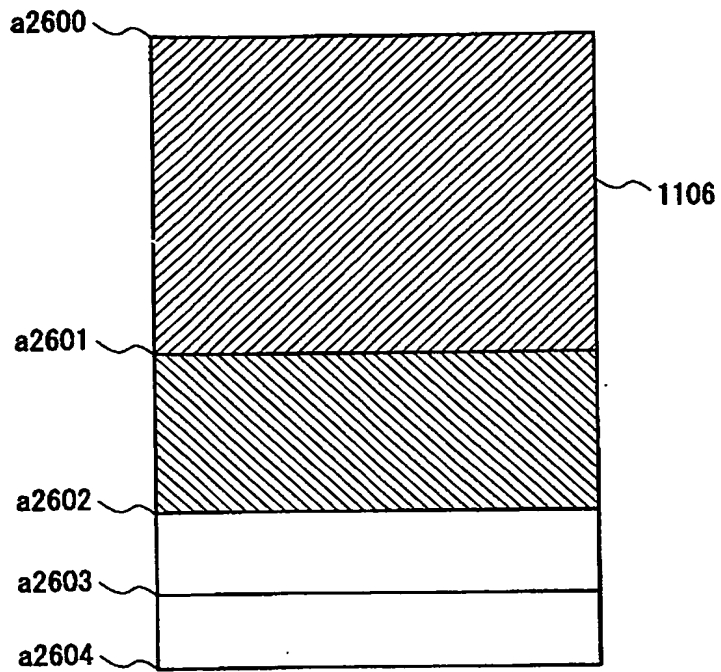
【図 10】



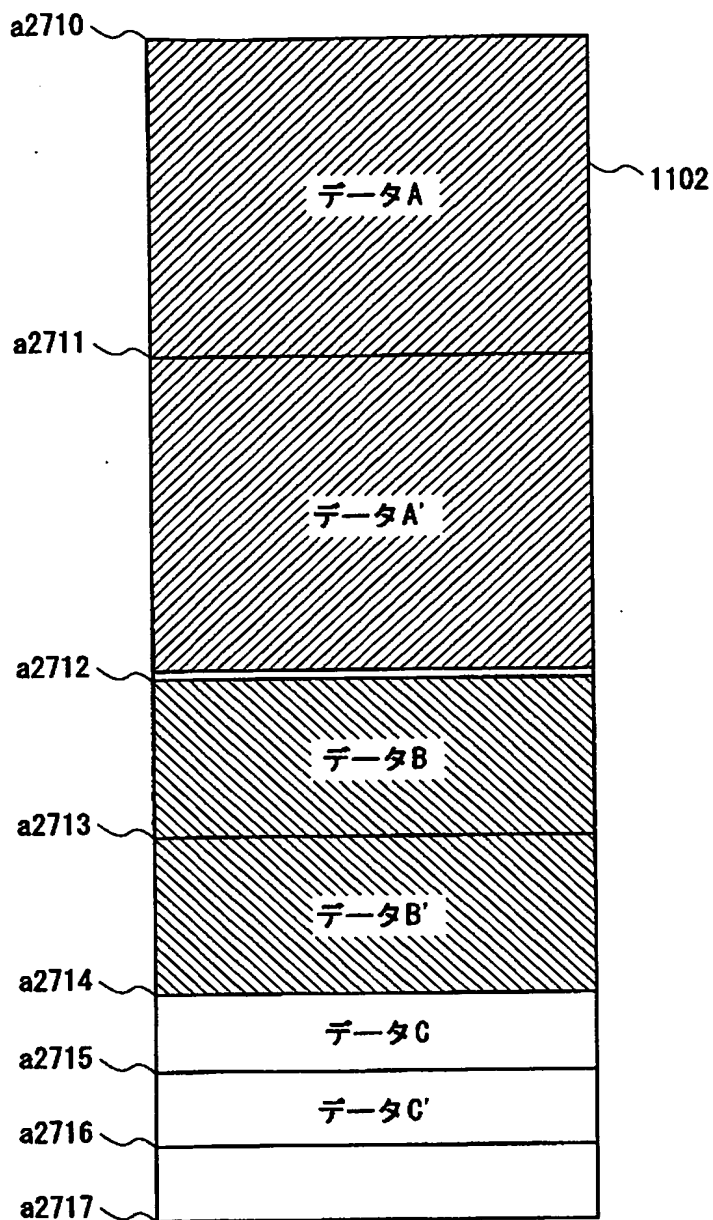
【図11】



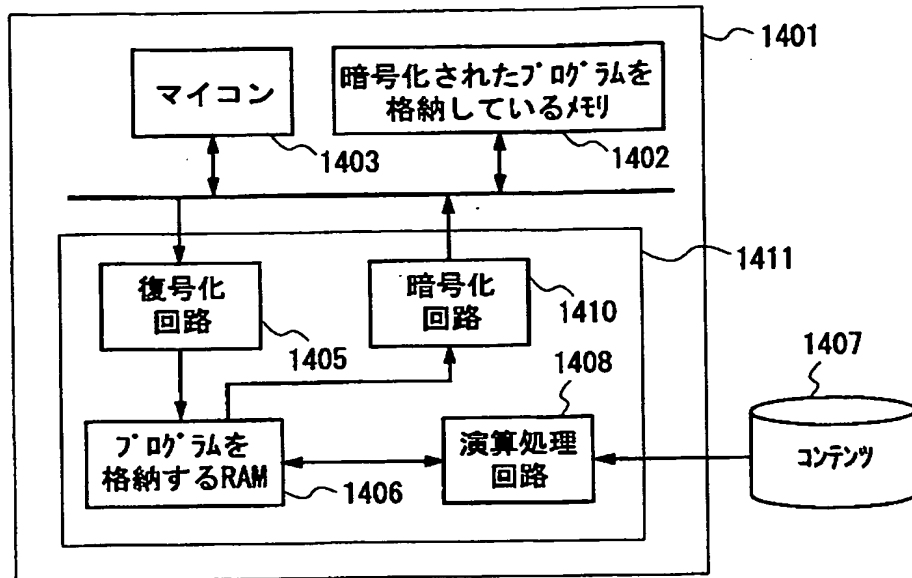
【図 12】



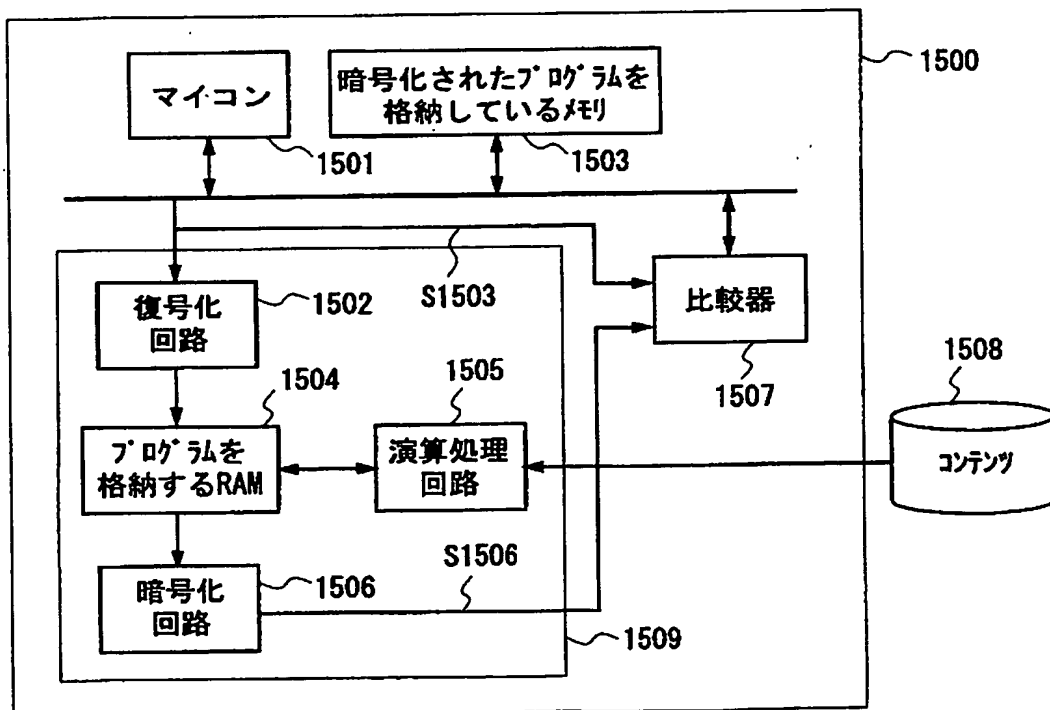
【図 13】



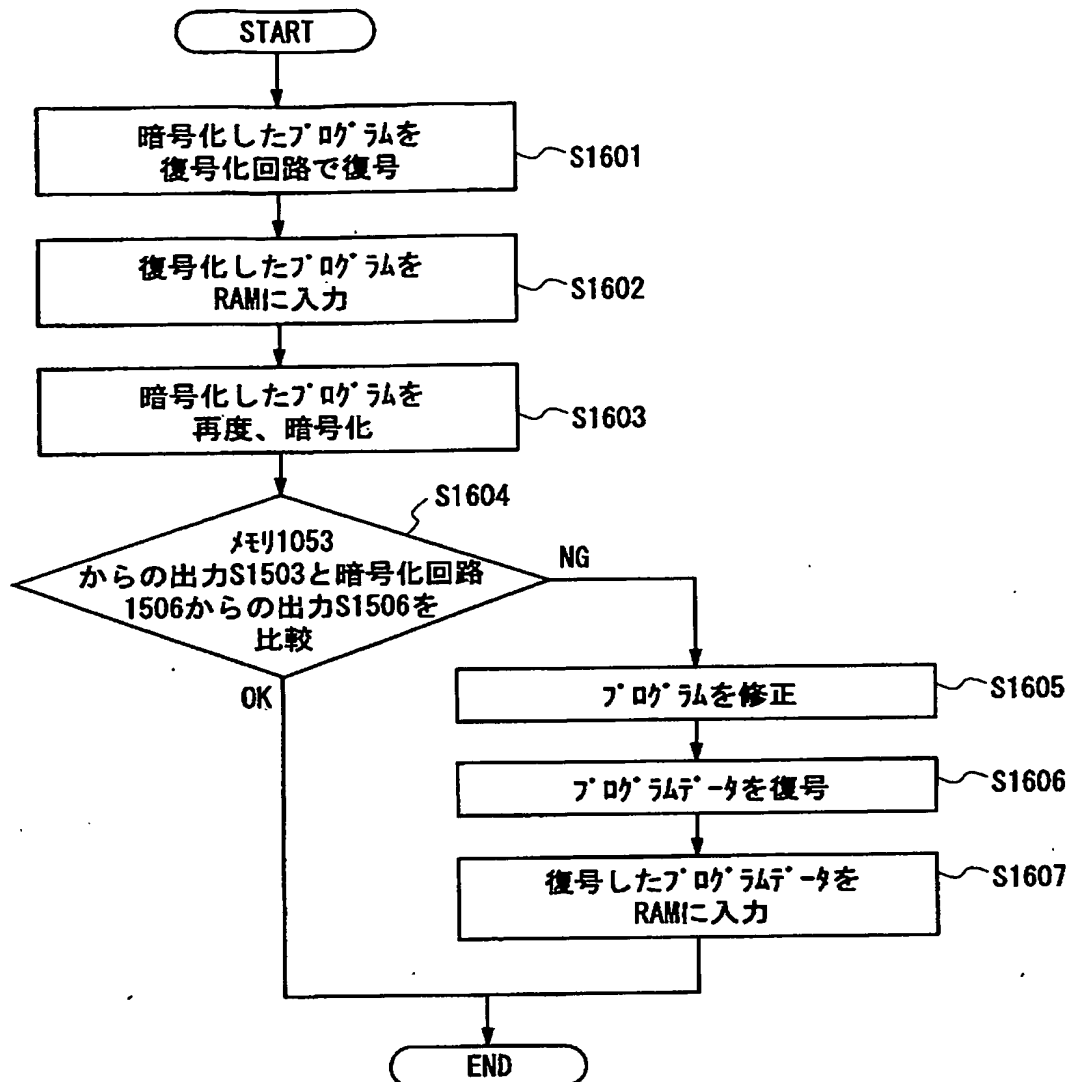
【図 14】



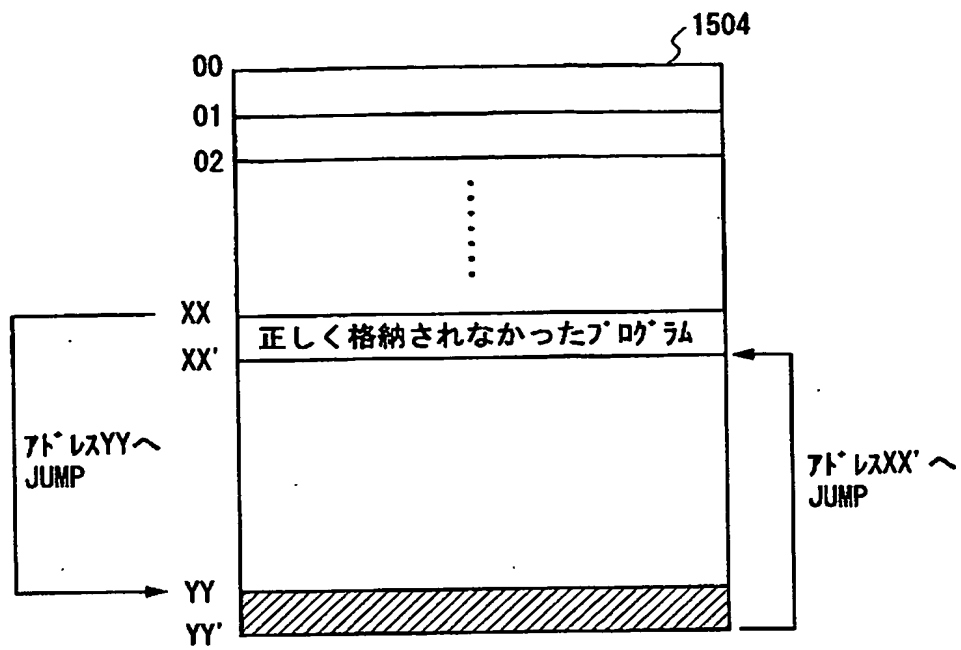
【図 15】



【図16】



【図 17】



【書類名】 要約書

【要約】

【課題】 DSPやCPUなどの演算処理ユニットのプログラムを外部からダウンロードする半導体集積回路装置において、半導体集積回路内にダウンロードした、第三者に漏洩したくない機密情報である書き換えプログラムを、その機密を保持しながら該書き換えプログラムが正しくダウンロードできたか否かの確認を可能とする半導体集積回路装置を提供する。

【解決手段】 ダウンロードした書き換えプログラムの内容を検証する回路、及び／またはダウンロードした書き換えプログラムの内容を検証するプログラムを備える。

【選択図】 図15

特願 2002-174883

出 願 人 履 歴 情 報

識別番号

[000005821]

1. 変更年月日

1990年 8月28日

[変更理由]

新規登録

住 所

大阪府門真市大字門真1006番地

氏 名

松下電器産業株式会社